EXHIBIT 3

Trials@uspto.gov Paper 9
571-272-7822 Entered: August 7, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETFLIX, INC.,
Petitioner,

v.

LAURI VALJAKKA,
Patent Owner.

IPR2023-00423
Patent 10,726,102 B2

Before GREGG I. ANDERSON, CHARLES J. BOUDREAU, and RUSSELL E. CASS, *Administrative Patent Judges*.

BOUDREAU, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Netflix, Inc. ("Petitioner") filed a Petition requesting *inter partes* review of claims 10 and 11 of U.S. Patent No. 10,726,102 B2 (Ex. 1001, "the '102 patent"). Paper 2 ("Pet."). Lauri Valjakka ("Patent Owner") filed a Preliminary Response. Paper 6 ("Prelim. Resp.").

We have authority to determine whether to institute an *inter partes* review. 35 U.S.C. § 314(b) (2018); 37 C.F.R. § 42.4(a) (2023). We may not institute an *inter partes* review "unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a).

Upon consideration of the arguments and evidence presented, we determine that Petitioner has not established a reasonable likelihood that it would prevail with respect to either claim challenged in the Petition. We therefore deny institution of *inter partes* review.

II. BACKGROUND

A. Real Parties in Interest

Petitioner and Patent Owner identify themselves as the real parties in interest. Pet. 75; Paper 3, 2 (Patent Owner's Mandatory Notices).

B. Related Matters

The parties advise us that the '102 patent is or has been involved in the following district court proceedings: *Valjakka v. Netflix, Inc.*, No. 4:22-cv-01490-JST (N.D. Cal.); *Valjakka v. Amazon.com, Inc.*, No. 6:21-cv-00945 (W.D. Tex.); *Valjakka v. Charter Communications, Inc.*, No. 6:22-cv-00491 (W.D. Tex.) (dismissed); *Valjakka v. Comcast Corp.*, No. 6:22-cv-00493 (W.D. Tex.) (dismissed); *Valjakka v. Meta Platforms, Inc.*, No. 6:22-cv-00495 (W.D. Tex.) (dismissed); *Valjakka v. Zoom Video Communications, Inc.*, No. 6:22-cv-00496 (W.D. Tex.) (dismissed); and

Valjakka v. Cox Communications, Inc., No. 6:22-cv-00497 (W.D. Tex.) (dismissed). Pet. 75; Paper 3, 2.

C. The ’102 Patent

The ’102 patent is titled “Method of and System for Providing Access to Access Restricted Content to a User” and relates to “using digital rights management keys to provide access to access restricted content.” Ex. 1001, code (54), 1:7–9. The access restricted content is digital media, e.g., text, audio, video, graphics, animations, or images. *Id.* at 5:48–51.

Figure 4 of the ’102 patent is reproduced below.

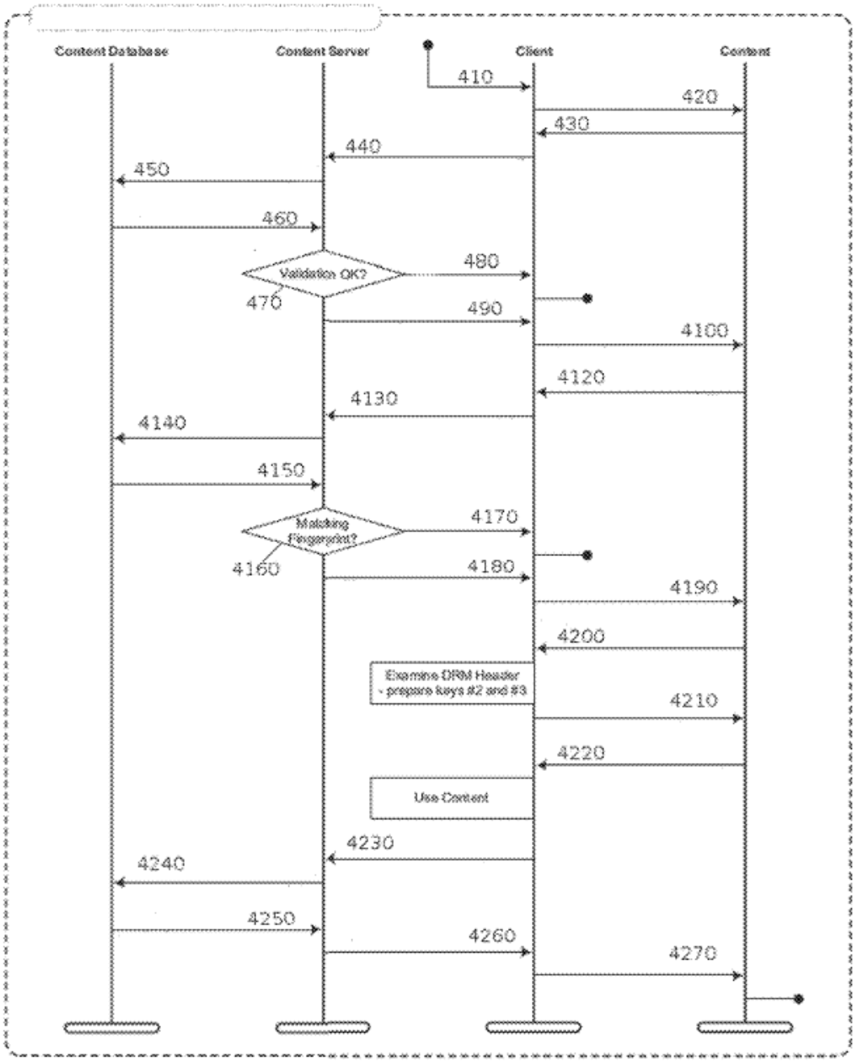

FIGURE 4

Figure 4, above, is a flow graph of a method of providing access to access restricted content to a user. Ex. 1001, 4:50–52. On the vertical axes, from left to right, are a content database, a content server, a client, and content. *Id.* at 10:3–4. The method begins in step 410 and proceeds to step 420 when the client locates content, e.g., by searching with a keyword. *Id.* at 10:4–7. In response, the client receives a content identifier (step 430). *Id.* at 10:7–9. The client transmits a message (e.g., a content request) comprising the content identifier received in step 430 and an identifier of the client to the content server (step 440). *Id.* at 10:9–13. The content server then sends a query comprising the content identifier and client identifier to the content database (step 450). *Id.* at 10:13–16.

Responsive to the query, the content database returns a validation result (e.g., whether the client has access to the requested content) to the content server (step 460). Ex. 1001, 10:18–21. If the validation was unsuccessful (e.g., the client does not have access to the requested content), processing ends (step 480). *Id.* at 10:21–25. If validation was successful, the message in step 460 comprises a first digital rights management (DRM) key and the content server transmits the first DRM key to the client (step 490). *Id.* at 10:25–29.

Using the first DRM key, the client may access the content (step 4100). Ex. 1001, 10:30–32. According to the '102 patent, however, although the client has access to the content, the user is not yet able to use the content. *Id.* at 7:35–38. Rather, the client must first obtain a fingerprint of the content based at least in part on the first DRM key (step 4120) and transmit the fingerprint to the content server, optionally with the content identifier (step 4130), for validation of the content fingerprint. *Id.* at 10:32–37. The content server then queries the content database for the content fingerprint, the query comprising the content identifier (step 4140), and in response, the content database provides the fingerprint to the content server (step 4150). *Id.* at 10:38–42. The server then compares the fingerprints received in steps 4130 and 4150 (step 4160). *Id.* at 10:42–43. In the case of a mismatch, processing ends (step 4170). *Id.* at 10:43–44. If the fingerprints match, the client is provided with a positive validation result (step 4180). *Id.* at 10:45–47. Responsive to the positive validation result, the client accesses the content to retrieve a DRM header (step 4190). *Id.* at 10:48–50. The client may optionally apply the first DRM key to the header, responsive to which the client gains access to an open DRM header of the content (step 4200). *Id.* at 10:50–52. Using the header, the client is enabled to prepare second and third DRM keys and apply at least one of the second and third DRM keys (step 4210) to retrieve the payload of the content (step 4220). *Id.* at 10:53–57.

D. Challenged Claims

Challenged claims 10 and 11 are reproduced below, reformatted from the ’102 patent and adopting Petitioner’s numbering of claim 10 elements for ease of reference. Claim 10 is independent.

> 10. [10P] A method, comprising:
>
> [10A] obtaining an access restricted content from at least one of a content database and a content providing server;
>
> [10B] obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query, the query comprising the content identifier and an identifier associated with the user;
>
> [10C] deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content wherein the obtaining is based at least in part on the first digital rights management key,

> [10D] causing the content providing server to validate the fingerprint, and, if the validation is successful, accessing the restricted content and information describing encryption properties of the access restricted content, and
>
> [10E] deriving, using the digital rights management header of the access restricted content, from the access restricted content a second and third digital rights management key,
>
> [10F] wherein the second and third digital rights management keys are applied to retrieve the payload of the access restricted content and
>
> [10G] wherein at least one of the second or third digital rights management key is used to encrypt the other key of the second or third digital rights management key,
>
> [10H] wherein the content is usable without being in an unprotected state.
>
> 11. The method of claim 10, wherein the first digital rights management key is unique to a specific session.

Ex. 1001, 14:1–30.

E. Evidence

Petitioner relies on the following prior art references in the asserted grounds of unpatentability:

Name	Reference	Exhibit
Downs	Downs et al., US 6,226,618 B1, issued May 1, 2001	1005
DeMello	DeMello et al., US 6,891,953 B1, issued May 10, 2005	1006
Schwartz	Schwartz et al., US 8,112,444 B2, issued February 7, 2012	1007
Walmsley	Walmsley et al., US 7,685,424 B2, issued March 23, 2010	1008

Pet. 1–2. Petitioner also relies on a Declaration of Paul D. Martin, Ph.D. (Ex. 1003).

F. Asserted Grounds

Petitioner asserts that claims 10 and 11 are unpatentable under 35 U.S.C. § 103 on the following grounds (Pet. 2):

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
10	103	Downs
10, 11	103	DeMello, Schwartz, Walmsley

III. ANALYSIS

A. Legal Standards

"In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable." *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (2012) (requiring *inter partes* review petitions to identify "with particularity . . . the evidence that supports the grounds for the challenge to each claim")). This burden of persuasion never shifts to the patent owner. *See Dynamic Drinkware, LLC v. Nat'l Graphics*, Inc., 800 F.3d 1375, 1378 (Fed. Cir. 2015) (discussing the burden of proof in *inter partes* review).

A patent claim is unpatentable for obviousness "if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains." 35 U.S.C. § 103.

> The ultimate determination of obviousness is a question of law, but that determination is based on underlying factual findings. . . . The underlying factual findings include (1) "the scope and content of the prior art," (2) "differences between the prior art and the claims at issue," (3) "the level of ordinary skill in the pertinent art," and (4) the presence of secondary considerations of nonobviousness such "as commercial success,

> long felt but unsolved needs, failure of others," and unexpected results.

In re Nuvasive, Inc., 842 F.3d 1376, 1381 (Fed. Cir. 2016) (citing *inter alia Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966)).

B. Level of Ordinary Skill in the Art

Petitioner contends that "[a] person having ordinary skill in the art ('POSITA') at the time of the alleged invention of the challenged claims would have had a bachelor's degree in computer science or computer engineering, and two to four years of experience in digital rights management and/or data security." Pet. 14 (citing Ex. 1003 ¶ 53). Petitioner further contends that "[s]ignificantly more practical experience could also qualify one not having the aforementioned education as a person of ordinary skill in the art while, conversely, a higher level of education could offset a lesser amount of experience." *Id.*

Patent Owner "adopt[s] Petitioner's proffered level of ordinary skill in the art because it comports with the technology and claims of the '102 Patent as well as the asserted prior art." Prelim. Resp. 7.

Based on our review of the record at this stage, we find Petitioner's assessment to be consistent with the level of skill reflected in the prior art references of record. *See Daiichi Sankyo Co. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007) (listing the type of problems encountered in the art, prior art solutions to those problems, and the sophistication of the technology as factors that may be considered in determining the level of ordinary skill in the art). Accordingly, we adopt Petitioner's articulation of the level of ordinary skill in the art.

C. Claim Construction

We interpret claim terms

> using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.

37 C.F.R. § 42.100(b) (2021).

1. "Fingerprint"

Petitioner contends that the term "fingerprint" should be construed as "a bit string, derived (or computed) directly from the content, that uniquely represents the content." Pet. 15–16 (citing Ex. 1003 ¶¶ 55–57; Ex. 1005, 14:13–14; Ex. 1008, 10:3–5; Ex. 1012 ¶ 720; Ex. 1013, 14). Patent Owner adopts Petitioner's construction. Prelim. Resp. 7. To the extent necessary for purposes of this Decision, we also adopt Petitioner's construction.

2. Order of Steps

Petitioner contends that "claim 10 imposes an ordering of at least steps [10B]-[10G]." Pet. 16–17 (ordering steps [10B]–[10G] in the order in which they appear in claim 10). According to Petitioner, "[t]his interpretation is consistent with the first method described in the specification." *Id.* at 18 (citing Ex. 1001, 10:35–37, 10:42–57; Ex. 1003 ¶ 60). Petitioner further contends that Petitioner's construction is consistent with the construction adopted by the Court in the co-pending District Court litigation—that "[t]he DRM Keys must be obtained or derived before restricted content is obtained" and "the first DRM key must be obtained and fingerprint validated before the second and third DRM keys are derived." Pet. 18–19 (citing Ex. 1013, 13; Ex. 1003 ¶ 61). Patent Owner adopts

Petitioner's construction. Prelim. Resp. 7. To the extent necessary for purposes of this Decision, we also adopt Petitioner's construction.

D. Obviousness of Claim 10 over Downs

Petitioner alleges claim 10 would have been obvious over Downs, relying in part on Dr. Martin's Declaration. Pet. 19–39 (citing Ex. 1003 ¶¶ 77–93). Patent Owner responds. Prelim. Resp. 20–28.

We begin our analysis with an overview of Downs, and we then address the parties' contentions with respect to the challenged claims.

1. Downs

Downs, titled "Electronic Content Delivery System," relates to electronic commerce and "the secure delivery and rights management of digital assets, such as print media, films, games, and music over global communications networks such as the Internet and the World Wide Web." Ex. 1005, code (54), 1:52–57. Downs discloses a method of securely providing encrypted data to a user's system. *Id.* at code (57).

Figure 6 of Downs is reproduced below.

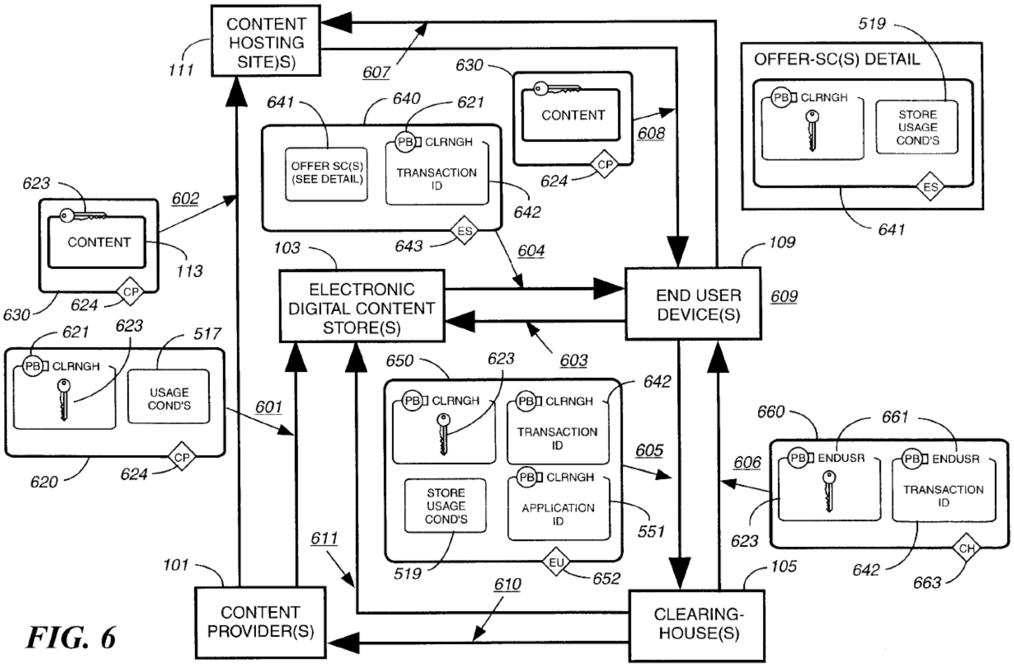

FIG. 6

Figure 6 of Downs, above, is a block diagram for a content distribution and licensing control system. Ex. 1005, 4:8–10. The system includes Content Provider(s) 101 or the proprietors of the Digital Content, Electronic Digital Content Store(s) 103, Intermediate Market Partners (not shown), Clearinghouse(s) 105, Content Hosting Site 111, Transmission Infrastructures 107, and End-User Device(s) 109. *Id.* at 8:55–65. Content Provider 101 "encrypts the Content 113 using an encryption symmetric key locally generated, and encrypts the Symmetric Key 623 using the Clearinghouse's 105 public key 621." *Id.* at 23:30–33. Content Provider 101 packs "encrypted Content 113, digital content-related data or metadata, and encrypted keys" in secure containers (SCs). *Id.* at 9:48–51. For example, the encrypted symmetric key, metadata, and other information about Content 113 are "packed into a Metadata SC" and encrypted content 113 and metadata are packed into a Content SC. *Id.* 18:1–67, 23:33–37. "There is one Metadata SC(s) 620 and one Content SC(s) 630 for every Content 113 object." *Id.* at 23:37–39. Content SC 630 is sent to content Hosting Site 111, which can reside at either Content Provider 101, Clearinghouse 105, or a special location dedicated for Content Hosting. *Id.* at 23:44–45. Metadata SC 620 associated with the content is distributed to "one or more Electronic Digital Content Store(s) 103." *Id.* at 23:42–44.

After completion of the purchase of content by the End-User Device, "Electronic Digital Content Store(s) 103 creates and transfers to the End-User Device(s) 109 a Transaction SC(s) 640." Ex. 1005, 23:57–61. Transaction SC 640 "includes a unique Transaction ID 535, the purchaser's name (i.e., End-User(s)') (not shown), the Public Key 661 of the End-User Device(s) 109, and the Offer SC(s) 641 associated with the purchased Content 113." *Id.* at 23:62–65.

Upon receipt of Transaction SC 640, End-User Device 109 "solicits license authorization from the Clearinghouse(s) 105 by means of an Order SC(s) 650." Ex. 1005, 24:5–9. Upon receipt of Order SC 650 from the End-User Device, Clearinghouse 105 verifies, for example, that Order SC 650 has not been altered and Transaction Data 642 and Symmetric Key 623 are complete and authentic. *Id.* at 24:17–32. If the verifications are successful, Clearinghouse 105 "decrypts the Symmetric Key 623 and the Transaction Data 642 and builds and transfers the License SC(s) 660 to the End-User Device(s) 109." *Id.* at 24:34–37.

Upon receipt of License SC 660, End-User Device 109 "requests the Content SC(s) 630 (step 607) from a Content Hosting Site(s) 111." Ex. 1005, 24:48–52. "Upon arrival of the Content SC(s) 630 (step 608), the End-User Device(s) 109 decrypts the Content 113 using the Symmetric Key 623 (step 609), and passes the Content 113 and the Transaction Data 642 to the other layers for license watermarking, copy/play coding, scrambling, and further Content 113 processing." *Id.* at 24:52–57.

2. *Independent Claim 10*

a. *Petitioner's Contentions*

i. *[10P] "A method, comprising"*

For the preamble of claim 10, Petitioner cites Downs's disclosure of "a method . . . of securely providing data to a user's system." Pet. 26 (quoting Ex. 1005, code (57)) (citing Ex. 1003 ¶ 77).

ii. *[10A] "obtaining an access restricted content from at least one of a content database and a content providing server"*

Petitioner cites Downs's disclosure that Content Provider 101 "owns the rights to the Content 113" and "use[s] tools provided as part of the

Secure Digital Content Electronic Distribution System 100 in order to prepare . . . Content 113 and related data for distribution." Pet. 26 (quoting Ex. 1005, 9:15–18, 48:29–31). Petitioner further cites Downs's disclosure that the "data related to the Content 113" includes metadata. *Id.* (quoting Ex. 1005, 9:21–26). Petitioner further cites Downs's disclosure that Content Provider 101 "encrypts the Content 113 using an encryption symmetric key locally generated." *Id.* (quoting Ex. 1005, 23:30–31). Petitioner contends that "[t]he content and its associated metadata are therefore '*access restricted content*.'" *Id.* (citing Ex. 1003 ¶ 78).

Petitioner contends that "[e]ncrypted content is packed with metadata into a Content SC and distributed to a Content Hosting Site 111," which provides requested content to End-User Device 109. Pet. 27 (citing Ex. 1005, 24:48–57). According to Petitioner, "[a] POSITA would understand that Content Hosting Site 111 . . . is a '*content providing server*' because it serves content to requesting End-User Devices." *Id.* at 27–28 (citing Ex. 1003 ¶ 79). Thus, argues Petitioner, "End-User Device 109 '*obtain[s] an access restricted content from at least one of a content database and a content prov[id]ing server*.'" *Id.* at 28 (bold emphasis omitted).

iii. [10B] "obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query, the query comprising the content identifier and an identifier associated with the user"

With respect to the recited "query," Petitioner cites Downs's disclosure that "End-User Device(s) 109 initiates the request for a Content SC(s) 630 by sending the License SC(s) 660 to the Content Hosting Site(s) 111." Pet. 29 (quoting Ex. 1005, 69:40–42). Petitioner further cites

Downs's disclosure that License SC 660 includes a "Content ID" that, according to Downs, is "[a] part that defines a unique ID assigned to a Content 113 item." *Id.* (citing Ex. 1005, 29:30–31, 37:26–38:20). Petitioner further cites Downs's disclosure that, "[b]efore transmitting the Content SC(s) 630 to the End-User Device(s) 109," a "database . . . kept of all of the License SC IDs that have been used to download Content 113 . . . can be checked to ensure that the End-User Device(s) 109 only makes one request for each piece of Content 113 purchased." *Id.* (citing Ex. 1005, 70:4–10). Petitioner contends that "a POSITA would understand that the hosting device uses an identifier associated with the End-User device to assess whether only one request for the content has been made." *Id.* at 29–30 (citing Ex. 1003 ¶ 81). Petitioner argues that "[t]he request to the Content Hosting Site by the End-User Device for the purchased content is therefore '*a query*' that '*compris[es] the content identifier and an identifier associated with the user*.'" *Id.* at 30.

With respect to recited "first digital rights management key," Petitioner contends that "[t]he Content Hosting Site receiving the End-User request (the 'primary content site') makes the decision of which secondary site should be used to access the requested content" and that "a POSITA would understand that the primary content site (Content Hosting Site 111) retrieves the requested Content SC from the appropriate secondary content site for delivery to the End User." Pet. 30 (citing Ex. 1005, 69:51–54, 70:18–20, 70:22–24; Ex. 1003 ¶ 82). Petitioner cites Downs's disclosure that a digital certificate includes a "public key, the name of the person or entity, an expiration date, the name of the certification authority, and other information" and contends that the Content SC "includes the Certificate for the Content Provider." *Id.* at 30–31 (quoting Ex. 1005, 14:23–25) (citing

Table at 38:26–39:10). Petitioner contends that "[t]he Content Provider's public key and its associated private key (the Content Provider's asymmetric key pair) are the '*first digital rights management key*'" and that "[a] POSITA would understand that the Content SC is stored on the secondary content site in a content database because a database was a common structure used to store data prior to January 2014." *Id.* (citing Ex. 1003 ¶ 83; Ex. 1011, 80[1]). Petitioner thus argues that "[w]hen the primary content site (Content Hosting Site 111) requests the Content SC from the secondary content site, it obtains the Content SC including the '*first digital rights management key from a content database*' (content provider public key included in the certificate)." *Id.* at 31. Further, according to Petitioner, because "the request for the Content SC is based on the query received from the End-User device including the '*content identifier and an identifier associated with the user*,' and "Downs therefore discloses '*the obtaining is based in part on a query, the query comprising the content identifier and an identifier associated with the user*.'" *Id.* at 31–32.

iv. [10C] "deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content wherein the obtaining is based at least in part on the first digital rights management key"

Petitioner contends that Downs's "Content SC further includes the encrypted content and a digest of the encrypted content," the content digest produced by the Content Provider using a one-way hash algorithm. Pet. 32 (citing Ex. 1005, 14:6–9, 15:65–66, 16:8–10). Petitioner cites Downs's disclosure that, "[b]ecause of the properties of the one-way hash functions,

[1] Bill Rosenblatt et al., *Digital Rights Management* (2002).

one can think of a message digest as a fingerprint of the message." *Id.* (emphasis omitted) (quoting Ex. 1005, 14:13–14). Moreover, Petitioner contends, "[t]he Content SC digest is encrypted with the Content Provider's private key [the recited '*first digital rights management key*'] to produce the digital signature for the SC." *Id.* (alteration in original) (bold emphasis omitted) (citing Ex. 1005, 16:11–13). According to Petitioner, "the digital signature is a bit string and is a unique representation of the content derived directly from the content." *Id.* at 33 (citing Ex. 1003 ¶ 84). Petitioner asserts that "[t]he digital signature is '*a fingerprint of the access restricted content*' that is '*derived, using the first digital rights management key, from the access restricted content, wherein the obtaining* [deriving] *is based at least in part on the first digital rights management key*.'" *Id.* at 32–33.

v. [10D] "causing the content providing server to validate the fingerprint, and, if the validation is successful, accessing the restricted content and information describing encryption properties of the access restricted content"

With respect to the limitation of "causing the content providing server to validate the fingerprint," Petitioner contends:

> Upon receipt of the Content SC, the Content Hosting Site (primary content site) verifies the integrity of the Content SC. As explained by Downs, "recipients of SC(s) can verify the integrity of the SC(s) and its parts by means of the received digital signature and part digests." (NF-1005, 14:3–5; *see also*, NF-1005, 25:14–18 ("Parties receiving the SC(s) can use the digital signature to verify all of the digests and thus validate the integrity and completeness of the SC(s) and all of its parts").) Specifically, the Content Hosting Site "decrypts the SC(s) digital signature" using the Content Provider's public key. (NF-1005, col. 16 (step 410).) The recipient runs the concatenation of the received content digest through the same hash algorithm used by the Content Provider to compute the SC digest. (NF-1005,

> col. 16 (step 411).) The Content Hosting Site then compares the computed Content SC digest with the one recovered from the Content Provider's digital signature. (NF-1005, col. 16 (step 412).) "If they are the same, recipient confirms that the received digests have not been altered." (NF-1005, col. 16 (step 412).)

Pet. 33. Thus, Petitioner argues that Downs's "system '*caus[es] the content providing server to validate the fingerprint*' . . . to verify the integrity of the received Content SC." *Id.* (citing Ex. 1003 ¶ 85).

With respect to the limitation "if the validation is successful, accessing the restricted content and information describing encryption properties of the access restricted content," Petitioner contends that, "[u]pon purchase of the content, the Clearinghouse provides the License SC to the End-User Device," and "the End-User Device requests the Content SC from the Content Hosting Site 111 using the License SC." Pet. 34; *see id.* at 24–25 (citing Ex. 1005, 24:5–9, 24:17–32, 24:34–37, 24:48–52), 27 (citing Ex. 1005, 24:58–57). Petitioner further contends that "[i]f the integrity of the Content SC is verified by the Content Hosting Site 111 (primary content site), the Content SC is transmitted to the End User Device 109" and that "[t]he End-User Device therefore has both the License SC and Content SC associated with the requested content." *Id.* at 35 (citing Ex. 1005, 70:4–6; Ex. 1003 ¶ 87). According to Petitioner, the End-User Device accesses the License SC received from the Clearinghouse to play the content received from the Content Hosting Site. *Id.* (citing Ex. 1005, 28:4–5). Petitioner cites Downs's disclosure that "License SC(s) 660 carries the Symmetric Key 623 and the Transaction Data 642, both encrypted using the Public Key 661 of the End-User Device(s) 109." *Id.* (citing Ex. 1005, 24:37–40.) Petitioner contends that "the key description part of the License SC indicates the encryption algorithm used to encrypt the symmetric key for the content, the symmetric key algorithm, and the identifier of the key used to encrypt the content, metadata, and watermarking instructions." *Id.* (citing Ex. 1005, 37:26–38:20, Table at 37:36). This information in the Key Description Part, argues Petitioner, "is '*information describing the encryption properties of the access restricted content*.'" *Id.* (citing Ex. 1003 ¶ 88). Petitioner concludes,

> Because the End-User Device accesses the License SC to play the content in the received Content SC (received only after the fingerprint of the access restricted content is validated by the Content Hosting Site . . .), the End-User Device "*access[es] . . . information describing the encryption properties of the access restricted content*" if the "*validation*" of the integrity of the Content SC using the message digest ("*fingerprint*") is successful.

Id. at 35–36 (citing Ex. 1003 ¶ 88).

vi. [10E] "deriving, using the digital rights management header of the access restricted content, from the access restricted content a second and third digital rights management key"

Petitioner contends that "the License SC indicates in the Key Description Part that the symmetric key was encrypted using the 'EU Pub Key' which is the public key portion of the End User Device's asymmetric key pair." Pet. 36 (citing Ex. 1005, Table at 37:36). Petitioner argues that "[t]he Key Description Part is a '*digital rights management header of the access restricted content*' . . . because it is associated with access restricted content." *Id.* (citing Ex. 1003 ¶ 89; Ex. 1005, 29:19–24 (Content URL), 29:30–33 (Content ID), 37:58–60).

According to Petitioner, "[f]rom this '*header*' information, the End-User Device '*derives*' the associated private key portion of its asymmetric key pair (public/private keys) to use to decrypt the Symmetric Key." Pet. 36. Petitioner contends that "[t]he End-User's asymmetric key pair is collectively the '*second digital rights management key*.'" *Id.* at 36–37 (citing Ex. 1003 ¶ 89).

Petitioner further contends, "[u]sing the '*second digital rights management key*' (End-User Device's private key) and the information concerning the encryption algorithm provided in the Key Description Part of the License SC header, the End-User device decrypts the Symmetric Key for the content which is a '*third digital rights management key*.'" Pet. 37 (citing Ex. 1003 ¶ 90).

vii. [10F] "wherein the second and third digital rights management keys are applied to retrieve the payload of the access restricted content and"

[10G] "wherein at least one of the second or third digital rights management key is used to encrypt the other key of the second or third digital rights management key

Petitioner contends that Downs's "Symmetric Key ('*third digital rights management key*') is encrypted with the public key portion of the End User Device's asymmetric key pair ('*second digital rights management key*')," and that Downs accordingly "discloses '*at least one of the second or third digital rights management key is used to encrypt the other key of the second or third digital rights management key*.'" Pet. 37. (citing Ex. 1003 ¶ 90). Petitioner then cites Downs's disclosure that the End-User Device "decrypts the Content 113 using the Symmetric Key 623." *Id.* (quoting Ex. 1005, 24:54–55). In summary, Petitioner argues that, "[i]n Downs, the private key portion of the End-User's asymmetric key pair is applied to decrypt the Symmetric Key and the Symmetric Key is applied to decrypt the encrypted content in the Content SC (the recited '*access restricted content*')." *Id.* at 37–38. Petitioner thus contends that Downs's End-User Device "*access[es] the access restricted content and information describing encryption properties of the access restricted content*" and that "Downs teaches '*the second and third digital rights management keys are applied to retrieve the payload of the access restricted content*.'" *Id.* (citing Ex. 1003 ¶ 91).

viii. [10H] "wherein the content is usable without being in an unprotected state"

Petitioner contends that "[c]ontent not '*in an unprotected state*' is protected content" and that, "as written, this limitation recites the content is usable when the content is in a protected state (e.g., encrypted)." Pet. 38 (citing Ex. 1003 ¶ 92). According to Petitioner, "[a] POSITA would have understood that encrypted (protected) content is not directly useable by the client device" and that "[t]he client device must first decrypt the content." *Id.*

Petitioner further contends, "Should PO contend this limitation covers the circumstance where content is stored in encrypted form and then decrypted using a stored decryption key, such a process is (1) not disclosed in the '102 patent and (2) was extremely well-known for decades prior to the '102 patent." Pet. 38 (citing Ex. 1010, 31–32[2]; Ex. 1011, 80–84). Petitioner further argues that Downs discloses storing content in the End-User Device in encrypted form and decrypting the content in real-time when the content is consumed by a user. *Id.* at 39 (citing Ex. 1005, 82:20–39, 82:51–55, 83:16–17; Ex. 1003 ¶ 93).

[2] S.R. Subramanta & Byung K. Yi, *Digital rights management*, 25(2) IEEE Potentials 31–34 (2006).

b. Patent Owner's Contentions

i. "first digital rights management key"

Patent Owner contends that Downs fails to teach the recited "first digital rights management key." Prelim. Resp. 22–23. According to Patent Owner, the Content Provider's public key and its associated private key (i.e., asymmetric key pair) in Downs "are different keys." *Id.* at 22 (citing Ex. 1005, 13:49–14:14). In contrast, argues Patent Owner, the '102 patent's "'first digital rights management key' obtained from a database and used to derive a fingerprint of the access restricted content is the same key." *Id.* at 23.

ii. "deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content"

Patent Owner contends that the recited step of "deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content" must be performed by the client, and that Petitioner concedes as much. Prelim. Resp. 23–24 (citing Pet. 18). Patent Owner then contends that "Downs does not teach that 'deriving a fingerprint' is conducted by the client as required by claim 10." *Id.* at 24. Specifically, Patent Owner argues that creating and encrypting the Content SC digest to produce a digital signature for the SC is "conducted by the Content Provider, not by the client," in Downs. *Id.*

iii. "causing the content providing server to validate the fingerprint, and, if the validation is successful, accessing the access restricted content"

Patent Owner contends that "Petitioner equates [Downs's] 'Content Hosting Site' to [the] 'content providing server' of the '102 Patent." Prelim.

Resp. 25. Patent Owner further contends that "the Petition shows . . . validating the fingerprint is performed by recipients of SC(s), not by the 'Content Hosting Site'" in Downs. *Id.* (citing Pet. 33). According to Patent Owner, the "content providing server" that "validate[s] the fingerprint" in claim 10 is a sender sending contents to the user, rather than a recipient. *Id.*

Patent Owner further contends that "Downs does not disclose using the fingerprint of Content SC to determine 'if the validation is successful, accessing the access restricted content.'" Prelim. Resp. 26 (emphasis omitted). Rather, argues Patent Owner, Downs's "purpose of validating the fingerprint of Content SC is to verif[y] the integrity of the Content SC, not to determine accessing the access restricted content." *Id.* Patent Owner contends that Downs's Content Hosting Site "validates the fingerprint of License SC(s)" and "not Content SC(s) (corresponding to fingerprint of the access restricted content of the '102 Patent) in order to determine accessing the access restricted content." *Id.* at 26–27 (emphasis omitted) (citing Ex. 1005, 46:8–41, 69:40–48).

c. *Discussion*

Having considered the parties' respective arguments and evidence, we conclude that Petitioner has not established a reasonable likelihood that it would prevail in showing that claim 10 is unpatentable over Downs.

As presented above, Petitioner cites for the claim step of "obtaining a first digital rights management key from a content database" Downs's disclosure of retrieval of a Content SC that includes a digital certificate that in turn includes a content provider's public key, mapping the content provider's public key to the recited "first digital rights management key." Pet. 30–31. For the step of "deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content wherein the obtaining is based at least in part on the first digital rights management key," in contrast, Petitioner does not allege that the content provider's *public key* is used for the recited "deriving" of a fingerprint or that the fingerprint is obtained (or derived) based in any part on the public key. Rather, as Patent Owner points out, Petitioner instead contends that Downs produces a "digital signature" (which Petitioner maps to the recited "fingerprint") of the content using "the Content Provider's *private key*," which Petitioner shifts to relying upon as "the recited 'first digital rights management key.'" *Id.* at 32–33 (emphasis added); *see* Prelim. Resp. 22. Petitioner provides no explanation or justification for this shift, other than the conclusory assertion—repeated verbatim in Dr. Martin's declaration—that "[t]he Content Provider's public key and its associated private key (the Content Provider's asymmetric key pair) are the '*first digital rights management key*.'" Pet. 30–31 (citing Ex. 1003 ¶ 83).

Notwithstanding Petitioner's arguments, we agree with Patent Owner that the specification and the claims of the '102 patent reflect that the same "first digital rights management key" (or "first DRM key") is both "obtain[ed] . . . from a content database" and "us[ed] . . . [to derive] a fingerprint of the access restricted content," "which is distinct from the Content Provider's public key and its associated private key of Downs." Prelim. Resp. 23; *see, e.g.*, Ex. 1001, 10:25–37, claim 10. On the record before us, Petitioner has not sufficiently shown that Downs teaches or suggests obtaining "a first digital rights management key from a content database" and then using *that key* to "deriv[e] . . . a fingerprint of . . . access restricted content," as recited in claim 10.

3. Conclusion

For the reasons given, we are not persuaded that Petitioner has demonstrated sufficiently that limitations [10B] and [10C] of claim 10 are taught or suggested by Downs. We therefore determine that the Petition does not demonstrate a reasonable likelihood of prevailing on this obviousness challenge as to claim 10.

In view of the foregoing, we do not address Petitioner's analysis or Patent Owner's response to the other limitations of the claim.

E. Obviousness of Claims 10 and 11 over DeMello, Schwartz, and Walmsley

Petitioner alleges claim 10 would have been obvious over DeMello, Schwartz, and Walmsley, relying in part on Dr. Martin's Declaration. Pet. 39–74 (citing Ex. 1003 ¶¶ 123–152). Patent Owner responds. Prelim. Resp. 28–35.

We begin our analysis with overviews of DeMello, Schwartz, and Walmsley, and we then address the parties' contentions with respect to the challenged claims.

1. DeMello

DeMello, titled "Method and System for Binding Enhanced Software Features to a Persona," discloses a system for processing and delivery of electronic content, such as electronic books, wherein the content may be protected at multiple levels, from "level 1" (essentially "no protection") to "level 5" (the "strongest level of protection," wherein content "can only be opened by authenticated reader applications that are 'activated' for a particular user, thereby protecting against porting of a title from one person's reader (or readers) to a reader that is not registered to that person."). Ex. 1006, code (54), 4:41–48, 5:23–6:20. DeMello discloses an infrastructure "which supports the distribution of protected content in a digital rights management ('DRM') system." *Id.* at 1:60–62. DeMello describes a server architecture including "a retail site which sells content items to consumers, a fulfillment site which provides to consumers the content items sold by the retail site, and an activation site which enables consumer reading devices to use content items having an enhanced level of copy protection." *Id.* at code (57).

Figure 9 of DeMello is reproduced below.

FIG. 9

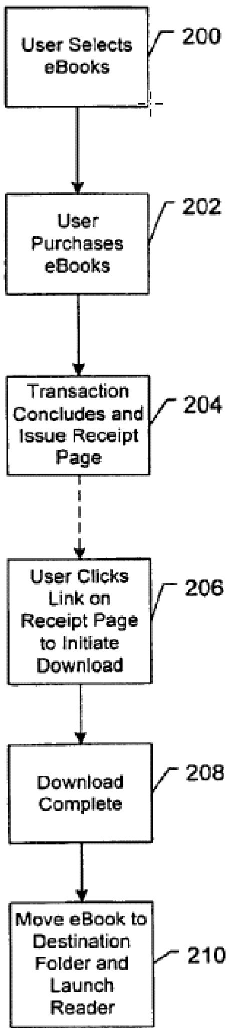
User Selects eBooks
200
User Purchases eBooks
202
Transaction Concludes and Issue Receipt Page
204
User Clicks Link on Receipt Page to Initiate Download
206
Download Complete
208
Move eBook to Destination Folder and Launch Reader
210

Figure 9, above, shows a "process by which eBook titles are acquired and delivered online," beginning in step 200 when a "user chooses book(s) via mechanism that the retail site implements." Ex. 1006, 25:66–67, 26:2–3. In step 204, when the transaction completes, the retail site generates a receipt page (i.e., an order confirmation or "thank you" page) that contains links (POST requests) for downloading each title purchased (i.e., the URLs containing the address of content server 76, plus the encrypted information created by URL encryption object 74). *Id.* at 26:4–11. For level 5 content, a client-side script executing at the user device "populate[s] the body of the POST with the activation certificate, preferably using COM object implemented by the reader which obtains the necessary activation certificate or relevant information therefrom." *Id.* at 26:4–15. When the user clicks on links in the POST message, the browser at the user's device initiates a download from content servers 76 (via download server ISAPI DLL 78). *Id.* at 26:16–18. For level 5 content, a license is generated and embedded in the LIT file, in addition to the Bookplate being created. *Id.* at 26:23–25. The license "contains the symmetric key 14A that encrypted the LIT file 'sealed' with the public key in the activation certificate," and "[w]hen the download is complete (step 208), the download server 76 logs the transaction and, on the client, the reader is launched automatically (step 210)." *Id.* at 26:25–30.

2. *Schwartz*

Schwartz, titled "Provisions for Validating Content Using a Content Registration Authority," describes a method "for facilitating the validation of content over a network." Ex. 1007, code (54), 4:62–64. Schwartz describes a central content registration authority that "registers the content disseminated by one or more content providers to one or more client devices." *Id.* at 5:44–46. According to Schwartz, "[a] client device which receives registered content can securely consume the content, based on an assumption that the content provider that furnished the content is entrusted by the content registration authority to provide the content." *Id.* at 5:46–52. A principal objective of Schwartz's system "is to prevent any entity from introducing malicious content into the system 300, e.g., via any content provider." *Id.* at 9:62–66.

Schwartz describes two strategies for improving content security. According to the second strategy (referred to as solution B), "registration may comprise storing the content identifier in a registration store maintained by the content registration authority." Ex. 1007, 5:66–6:2. Solution B is illustrated in Figure 5 of Schwartz, reproduced below.

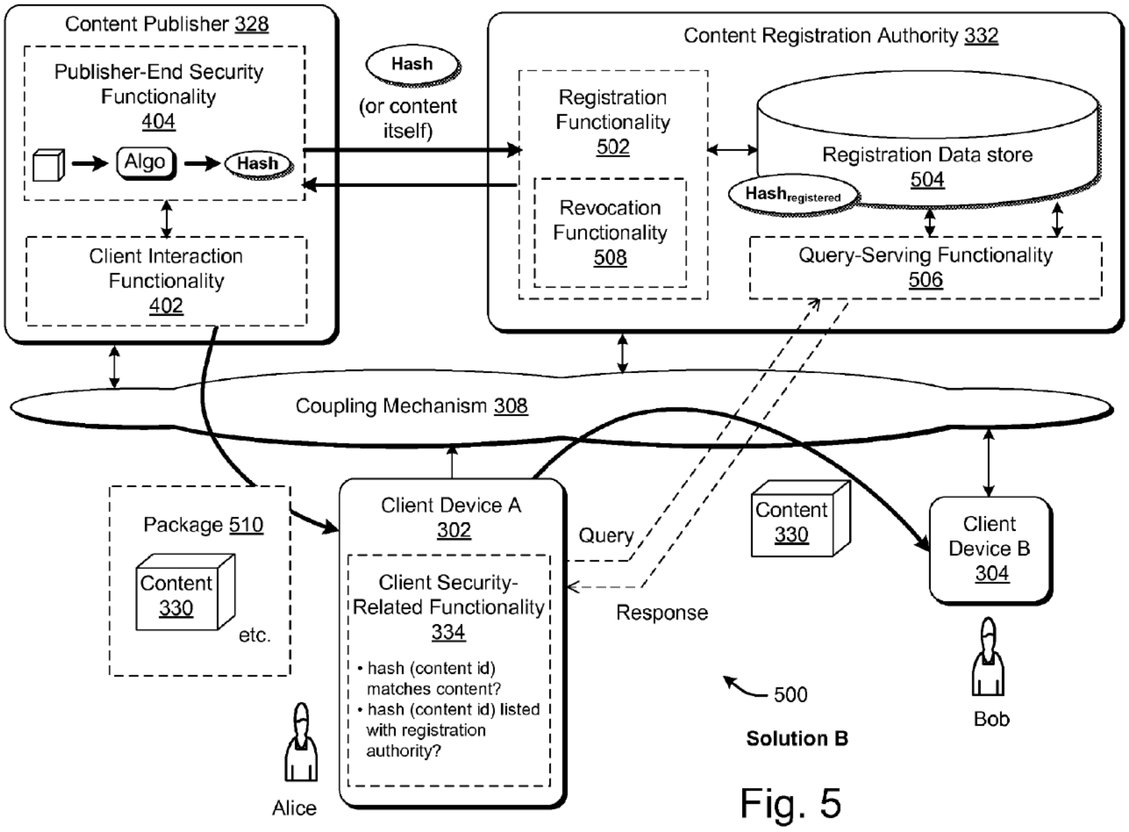
Content Publisher 328
Publisher-End Security Functionality 404
Algo
Hash
Client Interaction Functionality 402
Hash
(or content itself)
Content Registration Authority 332
Registration Functionality 502
Revocation Functionality 508
Registration Data store 504
Hash registered
Query-Serving Functionality 506
Coupling Mechanism 308
Package 510
Content 330
etc.
Client Device A 302
Client Security-Related Functionality 334
• hash (content id) matches content?
• hash (content id) listed with registration authority?
Query
Response
Content 330
Client Device B 304
Alice
Bob
500
Solution B

Fig. 5

With reference to Figure 5, above, the content registration authority "receive[s] a content identifier from the content publisher 328." *Id.* at 10:64–66. The content publisher 328 "form[s] the content identifier by computing a digest of the content 330, such as a hash of the content 330." *Id.* at 10:66–11:1. Content registration authority 332 then "store[s] the content identifier in a registration data store, thereby effectively registering the content identifier." *Id.* at 11:1–4. To verify the integrity of the content, the client device "independently compute[s] the content identifier of the received content 330, e.g., by forming a hash of the received content." *Id.* at 11:6–9. The client device "use[s] the computed content identifier as a key to determine whether the content has been previously registered in the registration data store of the content registration authority 332." *Id.* at 11:9–12. If the test passes, the client device "assesses that the content 330 is trustworthy." *Id.* at 11:12–16.

3. *Walmsley*

Walmsley, titled "Validating Untrusted Objects and Entities," discloses a validation method for determining whether an untrusted chip is valid. Ex. 1008, codes (54), (57). Walmsley describes the use of hash functions and explains that a "one-way hash function is not sufficient protection for a message." *Id.* at 11:43–44. According to Walmsley, a solution to this problem is a "Message Authentication Code, or MAC." *Id.* at 11:52–53. Walmsley discloses that use of hash-based MACs ("HMACs"), in particular, was "gaining acceptance as a solution for Internet message authentication security protocols." *Id.* at 12:32–34. An HMAC uses a "secret key shared by the two parties" to compute a hash. *Id.* at 12:32–47.

4. Independent Claim 10

a. Petitioner's Contentions

i. [10P] "A method, comprising"

For the preamble of claim 10, Petitioner cites DeMello's disclosure of a method including "delivery of electronic content wherein the content may be protected at multiple levels." Pet. 58 (quoting Ex. 1006, 4:41–43) (citing Ex. 1003 ¶ 129).

ii. [10A] "obtaining an access restricted content from at least one of a content database and a content providing server"

Petitioner cites DeMello's "ebook 10 contain[ing] content 16, which is text such as a book (or any electronic content) that has been encrypted by a key (the 'content key'), which itself has been encrypted and/or sealed" and contends that "[t]he encrypted content 16 is therefore '*access restricted content.*'" Pet. 59 (citing Ex. 1006, 6:38–42, Fig. 1; Ex. 1003 ¶ 130). According to Petitioner, "[a] user selects content (e.g., a book) via a mechanism implemented by a retail site selling content," and

> [w]hen the purchase transaction completes, the retail site generates "a receipt page (i.e., an order conformation or 'thank you' page) that contains links (POST requests) for downloading each title purchased (i.e., the URLs containing the address of content server 76, plus the encrypted information created by URL encryption object 74)."

Id. at 59–60 (quoting Ex. 1006, 26:4–11) (citing Ex. 1006, 26:2–3). Petitioner contends that "[w]hen the user clicks on the link provided in the POST message from the retail site, the browser at the user's device initiates a 'download from content servers 76 (via the download server ISAPI DLL 78).'" *Id.* at 61 (quoting Ex. 1006, 26:16–18). Petitioner argues that "[c]ontent server 76 at the Fulfillment Site is '*a content providing server*'" (*id.*) and that "the end-user device obtains the content from the content providing server at the Fulfillment Site" (*id.* at 63 (citing Ex. 1006, 27:39–50; Ex. 1003 ¶ 134)).

iii. [10B] "obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query, the query comprising the content identifier and an identifier associated with the user"

Petitioner cites a combination of DeMello, Schwartz, and Walmsley for this limitation. Pet. 64–66. Petitioner contends that, "[w]hile DeMello discloses the transmission of a content file having content encrypted using an encrypted symmetric key, DeMello does not provide a technique to authenticate that the received content is the actual content stored in the content database by the content provider" and "[a] POSITA would have therefore been motivated to add additional security to ensure the authenticity and integrity of the content retrieved by the end-user device and would have been led to Schwartz." *Id.* at 54–55 (citing Ex. 1003 ¶ 123).

In particular, Petitioner cites Schwartz's "solution B," in which content is downloaded to a client device and the client device "validat[es] the received content" by "contacting the query functionality 506 to determine whether there is a counterpart registered content identifier stored in the registration data store 504." Pet. 64 (quoting Ex. 1007, 25:47–52); *see* Ex. 1007, 25:44–46. Petitioner further cites Schwartz's disclosure that the client device "compute[s] a separately computed content identifier (based on the received content 330 itself) and use[s] this information as an index to determine whether the content has been previously registered in the data store 504." Pet. 64 (quoting Ex. 1007, 25:52–57). "If the test passes, the client device 'assesses that the content 330 is trustworthy.'" *Id.* at 52 (quoting Ex. 1007, 11:12–16). Petitioner indicates that Schwartz's content identifiers are formed "by computing a digest of the content 330, such as a hash of the content 330." *Id.* (quoting Ex. 1007, 10:66–11:1) (citing Ex. 1007, 11:6–9).

According to Petitioner,

> In the combined system of DeMello and Schwartz, the content store of DeMello uses a hash of the content as the Content ID (e.g., Book ID). (NF-1003, ¶124.) In the combined system, when the client device (e.g., DeMello's reader) receives content, the client device calculates the hash of the content and shares that value with the content registration authority (DeMello's content source) which validates the existence of the hash in its database. (*Id.*) If the hash exists, the client device confirms that the content provided by the content provider is the authentic content because any alternation of the content results in a different hash value than the value stored in the content store. (*Id.*) If the hash does not exist in the content store, the content has been altered in some way and the client terminates processing and does not access the content. (*Id.*) Thus, the combination of DeMello and Schwartz ensures that a client device (reader) uses only authentic content that has not been altered. (*Id.*)

Pet. 55–56. Petitioner states, "Schwartz discloses the use of a one-way hash function to calculate a content ID for content" but "does not disclose any details regarding the hash function used with its technique." *Id.* at 56.

Petitioner cites Walmsley's disclosure that "[a] one-way hash function is not sufficient protection for a message" because "one-way hash functions are susceptible to man-in-the-middle attacks." Pet. 57 (citing Ex. 1008, 11:42–47). Petitioner then cites Walmsley's HMAC, which Petitioner contends "uses a 'secret key shared by the two parties' to compute the hash." *Id.* at 54 (quoting Ex. 1008, 12:51) (citing Ex. 1008, 12:41–67; Ex. 1009, 455). Petitioner contends,

> [A] POSITA would have been motivated to integrate additional security into the hash to protect against attacks during transmission which would alter the value of the hash. . . . A POSITA would have therefore been motivated to use a hash derived from a cryptographic key such as the well-known HMAC to allow the receiving party to confirm the integrity of the hash and authenticate the hash came for the expected end-user device.

Id. at 56. Specifically, Petitioner contends that "[a] POSITA would have therefore been motivated to use Walmsley's MAC as the Content ID in Schwartz to provide integrity of the content ID when stored in the network (from Content Provider to Content Host) and when transmitted to the content provider for verification." *Id.* at 58; *see id.* at 65. Petitioner argues that "[t]he shared secret hash key is the '*first digital rights management key*.'" *Id.* at 66 (citing Ex. 1003 ¶ 138).

Petitioner notes that "Walmsley does not disclose that the symmetric hash key is shared by the content provider." Pet. 66. Petitioner contends,

> However, a POSITA would have understood that in the combined system the shared symmetric hash key for the content would have been included in the content file with the shared encryption key (content key) for the content because it is a cryptographic key used to process the content stored in the content store (database) of DeMello. (NF-1003, ¶139.) Like the content key, the shared hash key would have been sealed with the public key of the user's activation certificate. (*Id.*)

Id. (citing Ex. 1003 ¶ 139). Thus, argues Petitioner, "the client device '*obtain[s] a first digital rights management key from a content database*' . . . in the content file received by the user device" in the combination of DeMello, Schwartz, and Walmsley. *Id.*

iv. [10C] "deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content wherein the obtaining is based at least in part on the first digital rights management key"

Petitioner contends,

> In the combination of DeMello, Schwartz, and Walmsley, the client device "compute[s] a separately computed content identifier based on the received content 330 itself" as taught by Schwartz using the key-dependent one-way hash function, the HMAC, disclosed by Walmsley. (*See* NF-1007, 21:25-28.) The resulting key-hash value is a bit string and is unique representation of the content derived directly from the content—the recited "*fingerprint*." (NF-1003, ¶140.) Thus, the combination of DeMello, Schwartz, and Walmsley discloses "*deriving, using the first digital rights management key* [shared secret HMAC key], *from the access restricted content a fingerprint of the access restricted content* [the content identifier (keyed hash)] *wherein the obtaining is based at least in part on the first digital rights management key* [shared secret HMAC key]" [10C]. (*Id.*).)

Pet. 66–67.

v. [10D] "causing the content providing server to validate the fingerprint, and, if the validation is successful, accessing the restricted content and information describing encryption properties of the access restricted content"

Petitioner contends,

> The client device "use[s] the computed content identifier as a key to determine whether the content has been previously registered in the registration data store of the content registration." (NF-1007, 11:9–12.) That is, the user device transmits the keyed hash ("*fingerprint*") to the content registration database at the Fulfillment site, DeMello's content storage database ("*content database*"). (NF-1003, ¶141.) As taught by Schwartz, the content database at the Fulfillment Site ("*content providing server*") in the combined system validates

> the keyed hash by determining whether the keyed hash exists in the registration database of Content IDs. (*Id.*) If the keyed hash exists, the content received at the client device is authentic and has not been altered. (*Id.*) Thus, the combination teaches "*causing the content providing server to validate the fingerprint*" [10D]. (*Id.*)

Pet. 67.

Petitioner further contends that, "[i]f the content is determined to be authentic by the end-user device, the reader client is launched" and "the reader application accesses the content file." Pet. 68 (citing Ex. 1006, 6:11–16, 27:63–64). Petitioner argues that "DeMello therefore closes '*if the validation is successful, accessing the access restricted content.*'" *Id.* (citing Ex. 1003 ¶ 143).

Still further, Petitioner contends that DeMello's end-user device "includes additional 'code and data [that] are necessary to access "fully individualized" content on a given client device,'" including "an activation certificate having a public key and an encrypted private key" and "a program (e.g., a 'secure repository') that accesses the private key in the activation certificate by applying, in a secure manner, the key necessary to decrypt the encrypted private key." Pet. 70 (quoting Ex. 1006, 2:31–40) (citing Ex. 1006, 24:14–17, 25:9–11). Petitioner argues that "[t]his additional code and data is '*information describing encryption properties of the access restricted content*'" accessed if the validation is successful. *Id.* (citing Ex. 1003 ¶ 145).

vi. [10E] "deriving, using the digital rights management header of the access restricted content, from the access restricted content a second and third digital rights management key"

Petitioner cites DeMello's eBook content "that has been encrypted by a key (the 'content key'), which itself has been encrypted and/or sealed." Pet. 68 (quoting Ex. 1006, 6:39–42). Petitioner argues that "[t]he content key of DeMello is a '*second digital rights management key*.'" *Id.* at 68–69 (citing Ex. 1003 ¶ 144). Petitioner further argues that DeMello's content key is stored in license 14A in DRM storage portion 14 of the content file and that "[t]he DRM storage 14 portion of the content file 10 is a '*digital rights management header*.'" *Id.* at 69 (citing Ex. 1006, Fig. 1, 2:65, 6:48–53, 33:11–25; Ex. 1003 ¶ 144). Petitioner further argues that DeMello's "content key is sealed 'with the public key of the user's activation certificate'" and that "[t]he public key of the user's activation certificate and its associated private key (the asymmetric key pair for the activation certificate) are a '*third digital rights management key*.'" *Id.* (quoting Ex. 1006, 6:45–48) (citing Ex. 1003 ¶ 144).

vii. [10F] "wherein the second and third digital rights management keys are applied to retrieve the payload of the access restricted content and"

[10G] wherein at least one of the second or third digital rights management key is used to encrypt the other key of the second or third digital rights management key"

Petitioner cites DeMello's disclosure that the "secure repository uses its private key to decrypt the private key of the activation certificate, which, in turn, is then used to decrypt the symmetric key 14A of the eBook title, which, in turn, is used to decrypt the content stream 16 of the eBook title."

Pet. 70 (emphasis omitted) (quoting Ex. 1006, 24:19–23) (citing Ex. 1006, 6:36–7:2). Petitioner argues,

> Thus, the second digital rights management key (the symmetric key for the content) is encrypted using the third encryption key (the public key portion of the asymmetric key pair for the activation certificate). Accordingly, DeMello discloses "*deriving, using the digital rights management header of the access restricted content, from the access restricted content a second and third digital rights management key*" [10E], "*the second and third digital rights management keys are applied to retrieve the payload of the access restricted content*" [10F], and "*at least one of the second or third digital rights management key is used to encrypt the other key of the second or third digital rights management key*" [10G].

Id. at 71 (citing Ex. 1003 ¶ 146).

viii. [10H] "wherein the content is usable without being in an unprotected state"

Petitioner contends that "[c]ontent not '*in an unprotected state*' is protected content" and that, "as written, this limitation recites the content is usable when the content is in a protected state (e.g., encrypted)." Pet. 72 (citing Ex. 1003 ¶ 147). According to Petitioner, "[a] POSITA would have understood that encrypted (protected) content is not directly useable by the client device" and that "[t]he client device must first decrypt the content." *Id.*

Petitioner contends, "Should PO contend this limitation covers the circumstance where content is stored in encrypted form and then decrypted using a stored decryption key, such a process is (1) not disclosed in the '102 patent and (2) was extremely well-known for decades prior to the '102 patent." Pet. 72. Petitioner further contends that when DeMello's "reader device displays the content (e.g., the eBook), the reader must decrypt the content using the symmetric key provided in the license." *Id.* (citing

Ex. 1006, 27:66–67; Ex. 1003 ¶ 148). Petitioner argues, "[t]herefore, in DeMello, content is stored in the client device in encrypted form and decrypted in real-time when the content is consumed by the user." *Id.*

b. Patent Owner's Contentions

i. "obtaining a first digital rights management key from a content database"

Patent Owner contends that Petitioner's combination of DeMello, Schwartz, and Walmsley fails to teach limitations [10B] and [10C]. Prelim. Resp. 28. According to Patent Owner, Petitioner "admits" that "DeMello does not provide a technique to authenticate that the received content is the actual content stored in the content database," that Schwartz fails to teach a "first digital rights management key," and that Walmsley fails to teach "obtaining a first digital rights management key from a content database." *Id.* at 29–31 (citing Pet. 54–56, 66).

Patent Owner contends that, in Petitioner's proposed combination of DeMello, Schwartz, and Walmsley,

> the shared hash key . . . should not be sealed with the public key of the user's activation certificate in the content file received by the user device just like the content key of DeMello. Since the content key and the shared hash key have different functions, the content key is used to encrypt the content while the shared hash key is used to authenticate content, they require different processing methods.

Prelim. Resp. 31. Patent Owner further contends that "Walmsley teaches that the shared hash key is used to authenticate and stored within the authentication chip (corresponding to client's device of the '102 Patent) during a manufacturing/programming stage of the chip's life and must remain confidential." *Id.* at 31–32 (citing Ex. 1008, 26:45–52, 26:62–65).

Finally, Patent Owner contends,

> Thus, there is no need for the authentication chip "obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query" since the shared hash key is already stored in the authentication chip. Walmsley teaches away from "obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query."

Id. at 32.

ii. "causing the content providing server to validate the fingerprint, and, if the validation is successful, accessing the access restricted content"

Patent Owner contends that Petitioner's combination of DeMello, Schwartz, and Walmsley fails to teach limitation [10D]. Prelim. Resp. 33. According to Patent Owner, Petitioner "admits" that "DeMello does not provide a technique to authenticate that the received content is the actual content" and that Schwartz's "validating the fingerprint is conducted by the client device, not by the content registration database (corresponding to the content providing server of the '102 Patent)." *Id.* at 33–34 (citing Pet. 67). Patent Owner further contends that Petitioner does not cite Walmsley for the limitation of "causing the content providing server to validate the fingerprint." *Id.* at 34. Thus, Patent Owner contends that Petitioner's combination of DeMello, Schwartz, and Walmsley fails to teach "causing the content providing server to validate the fingerprint, and, if the validation is successful, accessing the access restricted content." *Id.*

iii. Hindsight

Patent Owner contends that "Petitioner has used hindsight to bridge the gaps in its argument." Prelim. Resp. 35.

c. Discussion

Having considered the parties' respective arguments and evidence, we conclude that Petitioner has not established a reasonable likelihood that it would prevail in showing that claim 10 is unpatentable over DeMello, Schwartz, and Walmsley.

First, Petitioner fails to map any teachings of DeMello, Schwartz, or Walmsley—individually or in combination—to the recitation "wherein the obtaining is based at least in part on a query, the query comprising the content identifier and an identifier associated with the user" in limitation [10B]. Indeed, Petitioner's only reference to a "query" in connection with this asserted ground is in Petitioner's quotation of Schwartz's disclosure that "[v]alidation for solution B comprises contacting the *query functionality 506* to determine whether there is a counterpart registered content identifier stored in the registration data store 504." Pet. 64 (emphasis added) (quoting Ex. 1007, 25:48–52). Petitioner, however, makes no showing how or why Schwartz's "query functionality 506" has any role in the step of "obtaining a first digital rights management key," as recited in limitation [10B]. The quoted sentence, moreover, relates to "[v]alidation," which, according to Petitioner's proposed claim construction prescribing an ordering of steps, occurs only after the step of "obtaining a first digital rights management key." *See supra* § III.C.2. Further, although the quoted sentence uses the identical term "content identifier," we find that Schwartz uses that term differently from the '102 patent, to refer to "a digest" or "a hash" of the content (*see, e.g.*, Ex. 1007, 5:57–61, 10:27–30, 11:6–9)—i.e., more akin to the "fingerprint" recited in claim 10.

Because Petitioner has not shown that the combination of DeMello, Schwartz, and Walmsley teaches or suggests a first digital rights management key being obtained "based at least in part on a query, the query comprising the content identifier and an identifier associated with the user," we are not persuaded by Petitioner's showing with respect to limitation [10B].

Second, we agree with Patent Owner that Petitioner has not made a sufficient showing that the combination of DeMello, Schwartz, and Walmsley teaches or suggests obtaining a first digital rights management key from a content database and then using that key to derive from access restricted content a fingerprint of that content, as recited in limitations [10B] and [10C]. *See* Prelim. Resp. 28–33. As Patent Owner points out, Petitioner recognizes that "DeMello does not provide a technique to authenticate that . . . received content is the actual content stored in the content data database by the content provider." Pet. 54–55 (quoted at Prelim. Resp. 28). Further, although Petitioner contends that a person of ordinary skill in the art would therefore have been led to Schwartz based on a motivation to ensure the authenticity and integrity of the content retrieved by end-user device, we find that Schwartz also fails to teach or suggest using a digital rights management key obtained from a content database to derive a fingerprint of access restricted content.

To be sure, Schwartz discloses that a content publisher and a client device each can compute a content identifier of received content, "e.g., by forming a hash of the received content" and that "[t]he client device . . . can then use the computed content identifier as a key to determine whether the content has been previously registered." Ex. 1007, 10:64–11:12. And as stated above, we find Schwartz's content identifier to be akin to the "fingerprint" of claim 10. Nonetheless, we find nothing in Schwartz suggesting that the content identifier is "deriv[ed] using [a] . . . key" that is "obtain[ed] . . . from a content database," as recited in limitations [10B] and [10C].

Further, notwithstanding Petitioner's contentions that "[i]n the proposed combination, a POSITA would have been motivated to use a keyed hash for computing the Content ID (e.g., Book ID) in the combination of DeMello and Schwartz as disclosed by Walmsley" and that "[s]pecifically, a POSITA would have been motivated to use Walmsley's message authentication code which is a 'key-dependent one-way hash function'" (Pet. 65 (citing Ex. 1003 ¶ 138; Ex. 1009, 455)), we find that the addition of Walmsley to the combination would at most suggest using a key to derive a fingerprint—not obtaining that key from a content database, as recited in limitation [10B]. Indeed, Petitioner acknowledges that "Walmsley does not disclose that the symmetric hash key is shared by the content provider." *Id.* at 66. While Petitioner further alleges that "a POSITA would have understood that in the combined system the shared symmetric hash key for the content would have been included in the content file with the shared encryption key (content key) for the content" because it is "a cryptographic key used to process the content stored in the content store (database) of DeMello" and that "[l]ike the content key, the shared hash key would have been sealed with the public key of the user's activation certificate" (*id.* (citing Ex. 1003 ¶ 139)), Petitioner's only support for those allegations are verbatim statements by Dr. Martin that provide no supporting factual evidence and are, as such, entitled to little or no weight (*see* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.")). We find more persuasive Patent Owner's argument that because "Walmsley teaches that the shared hash key is used to authenticate and stored within the authentication chip (corresponding to client's device of the '102 Patent) during a manufacturing/programming stage of the chip's life and must remain confidential" (Prelim. Resp. 31–32 (citing Ex. 1008, 26:45–52, 26:62–65)), there would be "no need for the authentication chip 'obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query' since the shared hash key [would] already [be] stored in the authentication chip" in the proffered combination (*id.*).

Third, we are not persuaded by Petitioner's showing for limitation [10D]. As set forth above, Petitioner contends with respect to that limitation that "the user device transmits the keyed hash ('fingerprint') to the content registration database at the Fulfillment site, DeMello's content storage database ('content database')" and that "[a]s taught by Schwartz, the content database at the Fulfillment Site ('content providing server') in the combined system validates the keyed hash." Pet. 67 (emphasis omitted). Petitioner similarly argues, in support of its alleged motivation to combine the teachings of DeMello and Schwartz, that, "[i]n the combined system, when the client device (e.g., DeMello's reader) receives content, the client device calculates the hash of the content and shares that value with the content registration authority (DeMello's content source) which validates the existence of the hash in its database." *Id.* at 55. As Petitioner itself appears to recognize, however, it is the client device in Schwartz, not the content registration authority, that performs the validation of the hash of the content to determine whether the content may be accessed. *See id.* ("If the hash exists, *the client device confirms that the content provided by the content provider is the authentic content* . . . .” (emphasis added)).

Schwartz expressly explains that, “[t]o verify the integrity of the content 330, the client device A 302 can independently compute the content identifier of the received content 330, e.g., by forming a hash of the received content” and that “*[t]he client device A 302 can then use the computed content identifier as a key to determine whether the content has been previously registered* in the registration data store of the content registration authority 332.” Ex. 1007, 11:6–16 (emphasis added); *see also id.* at Fig. 5 (illustrating “client security-related functionality 334” within client device A 302 determining whether “hash (content id) matches content?” and whether “hash (content id) [is] listed with registration authority?”), 12:45–50 (“The client security-related functionality 334 is assigned the task of . . . validating the content 330 . . . .”), 21:29–30 (referring to “validation of the content 330 by the client device A 302”), 25:43–57 (result of lookup is returned to the client device, and client A does the “validating” and “determin[ing]”).

Petitioner does not provide any persuasive reason that a person of ordinary skill in the art, when making the proffered combination, would have moved the locus of the hash-validation function from Schwartz’s client device to DeMello’s fulfillment site or content source as argued. Moreover, as Patent Owner points out, Petitioner does not rely on Walmsley for the recitation of “causing the content providing server to validate the fingerprint.” Prelim. Resp. 34. Because we find no teaching or suggestion of that recitation in the combination of DeMello, Schwartz, and Walmsley, we are not persuaded by Petitioner’s showing with respect to limitation [10D].

5. Dependent Claim 11

Claim 11 depends from claim 10 and therefore incorporates each of the limitations of claim 10. Accordingly, for the same reasons as provided for claim 10 (*see supra* § III.E.4), we accordingly determine that Petitioner also has failed to demonstrate a reasonable likelihood of prevailing on its challenge to claim 11 as obvious over DeMello, Schwartz, and Walmsley.

6. Conclusion

For the reasons given, we are not persuaded that Petitioner has demonstrated sufficiently that limitations [10B]–[10D] of claim 10 are taught or suggested by the combination of DeMello, Schwartz, and Walmsley. We therefore determine that the Petition does not demonstrate a reasonable likelihood of prevailing on this obviousness challenge as to independent claim 10 or dependent claim 11.

In view of the foregoing, we do not address Petitioner's analysis or Patent Owner's response to the other limitations of the claims.

IV. CONCLUSION

For the foregoing reasons, Petitioner has not demonstrated a reasonable likelihood of prevailing with respect to any claims. Thus, we do not institute an *inter partes* review.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Petition is *denied*, and no trial is instituted.

FOR PETITIONER:

Lori A. Gordon
Jassiem Moore
PERKINS COIE LLP
gordon-ptab@perkinscoie.com
moore-ptab@perkinscoie.com

FOR PATENT OWNER:

Jacob B. Henry
William P. Ramey, III
RAMEY LLP
jhenry@rameyfirm.com
wramey@rameyfirm.com